User Data Groups

Module Guide: User Data Groups

Module Location

Settings > Function Authorization > User Data Groups

Module Purpose

The **User Data Groups** module serves as a master data hub for creating and managing user groups (or roles) within the system. Instead of granting access rights one-by-one to each user, an administrator can create functional groups (such as "Customs," "KOKILA," "SUBCON"), add users to those groups, and then grant access rights to the group. This is a **Role-Based Access Control (RBAC)** approach that simplifies and standardizes system security. ?

1. Main View (List of User Groups)

The main page displays a list of all user groups that have been defined for a specific company.

View Explanation

- **Filter**: Allows searching for a specific group by **Group Name**.
- **User Group Table**:
  - **Group Name**: The unique name of the user group.

- **Group No**: An internal unique ID for the group.
- **Company Name**: Indicates the company where this group is defined and applies.

- **Action Buttons/Links**:
  - **[Add user group]**: A link to open the form and create a new user group.
  - **Search / Show all**: Buttons to perform a search or display all data again.

2. Steps to Create a User Group

Although the add form is not displayed, the workflow can be summarized as follows:

- From the main page, click the **[Add user group]** link.
- The system will open a new page where the user must enter a **Group Name** (e.g., "Accounting Staff," "Warehouse Manager," "Auditor").
- Select the **Company Name** where this group will be active.
- Click **Save**. The new group will then appear in the list on the main page.
- The next step after creating a group is to add users to it, which is likely done in another module (e.g., in the user management module).

3. Integrated Workflow & Business Process

- **Foundation of Security**: The groups created here are the foundation of the entire system security matrix.?

- **Bulk Access Granting**: After a group is created, an administrator can go to other authorization modules (such as **Function Authorization**, **Account Link Authorization**, **Verification Approval**) and grant access rights directly to a group. All users who are members of that group will automatically inherit the same access rights.?

- **Access Management Efficiency**: If a new employee joins, the administrator does not need to grant dozens of access rights manually. They simply add the employee to the appropriate group (e.g., "Purchasing Staff"), and the employee immediately gets all the necessary access for their role. Similarly, when an employee moves to a different department, the admin only needs to move them to a new group.

4. Tips & Important Notes

- Design the user group structure based on the functional roles and responsibilities in your company, not on individual names.?

- Use clear and intuitive group names.

- Managing user groups is a critical task that should be performed by a System Administrator or the IT department responsible for system security.

- Conduct regular audits of each group's membership to ensure no users have **excessive privileges**.

Revision #1
Created 23 October 2025 08:11:48 by Sayu
Updated 23 October 2025 08:14:19 by Sayu